IN THE SPECIFICATION

Please replace the paragraph beginning at page 7, line 8 of the original specification with the following replacement paragraph.

--Described herein is a technology facilitating rights enforcement of digital goods using watermarks. Also described herein is a fingerprinting technology for protecting digital goods by detecting collusion as a malicious attack and identifying the participating colluders[[.]]. With this technology, digital goods are protected by a mechanism that detects collusion and colluders. In other words, with this technology, digital goods are protected by identifying that a digital good has had its mark removed and who removed that mark. That way, piracy crimes can be more effectively investigated.--

Please replace the paragraph beginning at page 7, line 16 of the original specification with the following replacement paragraph.

--At least one implementation of the technology, described herein, is characterized by limited BORE-resistance at the protocol level. (BORE is "break once, run everywhere.") If a digital pirate breaks one client and enables this client to avoid watermark detection, all content (both marked/protected and ~~an~~ unmarked/free) can be played as unmarked only on that particular client. However, to enable other clients to play content as unmarked, the digital pirate needs to collude the extracted detection keys from many clients in order to create content that can evade watermark detection on all clients.--

Please replace the paragraph beginning at page 8, line 10 of the original specification with the following replacement paragraph.

--Since, with this technology, a watermark detector uses its assigned "fingerprint" (as part of the secret detection key) to detect a watermark embedded in a digital good, a ~~an~~ digital pirate (or group of such pirates) leaves her "fingerprint" when she removes (or modifies) the embedded watermark. Thus, like a burglar without gloves, the digital pirate leaves her fingerprints when she commits a crime.--

Please replace the paragraph beginning at page 13, line 11 of the original specification with the following replacement paragraph.

--Unlike conventional fingerprinting, the fingerprints are not embedded in the digital good in at least one implementation of the exemplary collusion resister. Rather, they are assigned to (or associated with) a "client." A client may be called a "detection entity" because it is an entity that may detect a watermark. Examples of a detection entity include a person, company, or other business entity. Alternatively, a "detection entity" may be a specific copy of an application (e.g., a media player), a hardware device ~~devices~~, or some combination. More specifically, the fingerprints are assigned to a watermark detector (WMD). In that implementation, the watermark detector uses its assigned [[a]] secret detection key—that key includes the fingerprint used to detect the watermark. The detection key is different from the embedding key. By gaining the knowledge of a small number of detection keys (through collusion or other means), a pirate cannot remove the marks from the protected digital good.--

Please replace the paragraph beginning at page 14, line 21 of the original specification with the following replacement paragraph.

--Only colluders with detection keys that belong to the same segment can participate in a collusion clique on that segment. Colluders with keys belonging ~~belong~~ to differing segments will be of no benefit to each other (unlike in conventional FP)[[.]]. With segmentation, the minimum collusion size K grows as $O(N \log N)$, where N is object size.--

Please replace the paragraph beginning at page 17, line 9 of the original specification with the following replacement paragraph.

--Fig. 1 illustrates the collusion-resistant architecture 100. The architecture includes a key generation ~~generations~~ entity 110, marker 120, fingerprint detector 130, and watermark detector 140. Although Fig. 1 also shows an attacker 150, the attacker, of course, is not part of the architecture. However, their actions are anticipated by this architecture.--